IPA Software Reliability Enhancement Center
Information-technology Promotion Agency, Japan

IPAセミナー【 第1部 】

組込みシステムの品質説明力強化に向けた仕組みづくり

2013年6月13日

独立行政法人 情報処理推進機構
技術本部　ソフトウェア高信頼化センター
ソフトウェアグループ・研究員　田中和夫

Copyright © 2013 IPA, All Rights Reserved

組織名称が変わりました

SEC
Software Reliability Enhancement Center

快適なくらしと豊かな社会を支える
情報処理システムの信頼性向上を目指して

独立行政法人情報処理推進機構　技術本部
ソフトウェア・エンジニアリング・センター

2013年6月1日から

独立行政法人情報処理推進機構　技術本部
ソフトウェア高信頼化センター (略称：SEC)

Software Reliability Enhancement Center

Copyright © 2013 IPA, All Rights Reserved

第三期中期計画（2013年度からの5年間）

SEC Software Reliability Enhancement Center

～重要インフラ分野等における情報処理システムの信頼性・安全性の向上～

1. 重要インフラ分野の情報処理システムに係るソフトウェア障害情報の収集・分析及び対策
   - ■ 重要インフラシステム等のソフトウェア障害情報の収集・分析
   - ■ 重要インフラシステム等のソフトウェア障害の再発防止の導入促進や事例に対する対策支援
2. 利用者視点でのソフトウェア信頼性の見える化の促進
   - ■ ソフトウェア品質説明力の強化の促進
   - ■ ソフトウェア信頼性の見える化促進のための環境整備
3. ソフトウェアの信頼性に関する海外有力機関との国際連携

Copyright © 2013 IPA, All Rights Reserved

本日の内容

SEC
Software Reliability Enhancement Center

- 背景
  - 一旦事故が起こると求められる品質説明
  - 複雑化・高度化でソフト起因の障害は増加傾向？
  - 利用者にもITリテラシーが求められるが…
- ソフトウェア品質説明とは？
  - 品質説明の要素
  - 説明力強化の３つの視点
- ソフトウェア品質説明のための制度ガイドライン
  - 目的・位置づけ
  - 制度ガイドラインの概要
  - 事例（PSQ認証制度）
- 今後の展開

Copyright © 2013 IPA, All Rights Reserved

（背景）
一旦事故が起こると求められる品質説明

Copyright © 2013 IPA, All Rights Reserved

日本製自動車の「意図しない急加速（UA）」

SEC Software Reliability Enhancement Center

NHTSA NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Enter Email Address SUBSCRIBE SEARCH Home

Sign up for Email Updates

DRIVING SAFETY | VEHICLE SAFETY | RESEARCH | DATA | LAWS & REGULATIONS | ABOUT NHTSA

About the Administrator

Calendar

Congressional Testimony

Print Share RSS Feed Email

U.S. Department of Transportation Releases Results from NHTSA-NASA Study of Unintended Acceleration in Toyota Vehicles

DOT 16-11
Tuesday, February 8, 2011
Contact: Olivia Alair

ed results from an
unintended acceleration in
n (NHTSA) launched the study
s with expertise in areas such
ference and software integrity to conduct new research into whether
in incidents of unintended acceleration.

ble of producing the large throttle openings required to create dangerous
al safety defects identified by NHTSA more than a year ago - "sticking"
dals to become trapped by floor mats - remain the only known causes for
has recalled nearly 8 million vehicles in the United States for these two

- 2009～2010年
  日本製自動車の「意図しない急加速」に関するクレームが急増
- 米国議会や米運輸省道路交通安全局（NHTSA）から報告を求められるもメーカ側は説明に苦慮
- NHTSAは米国航空宇宙局（NASA）に脆弱性の有無の調査を要請

出典：http://www.nhtsa.gov/PR/DOT-16-11

Copyright © 2013 IPA, All Rights Reserved

ＮＡＳＡ が実施したこと

SEC Software Reliability Enhancement Center

調査範囲

電子スロットル制御(Electronic Throttle Control)システムの設計及び/もしくは実装に実際に意図しない加速(Unintended Acceleration)を引き起こすことが予期できる脆弱性があるかないかを決定する。

- UAを引き起こす可能性はあるか
- 通常の使用で実際に起こりうるか

実施した解析（いずれもツールを最大限活用）

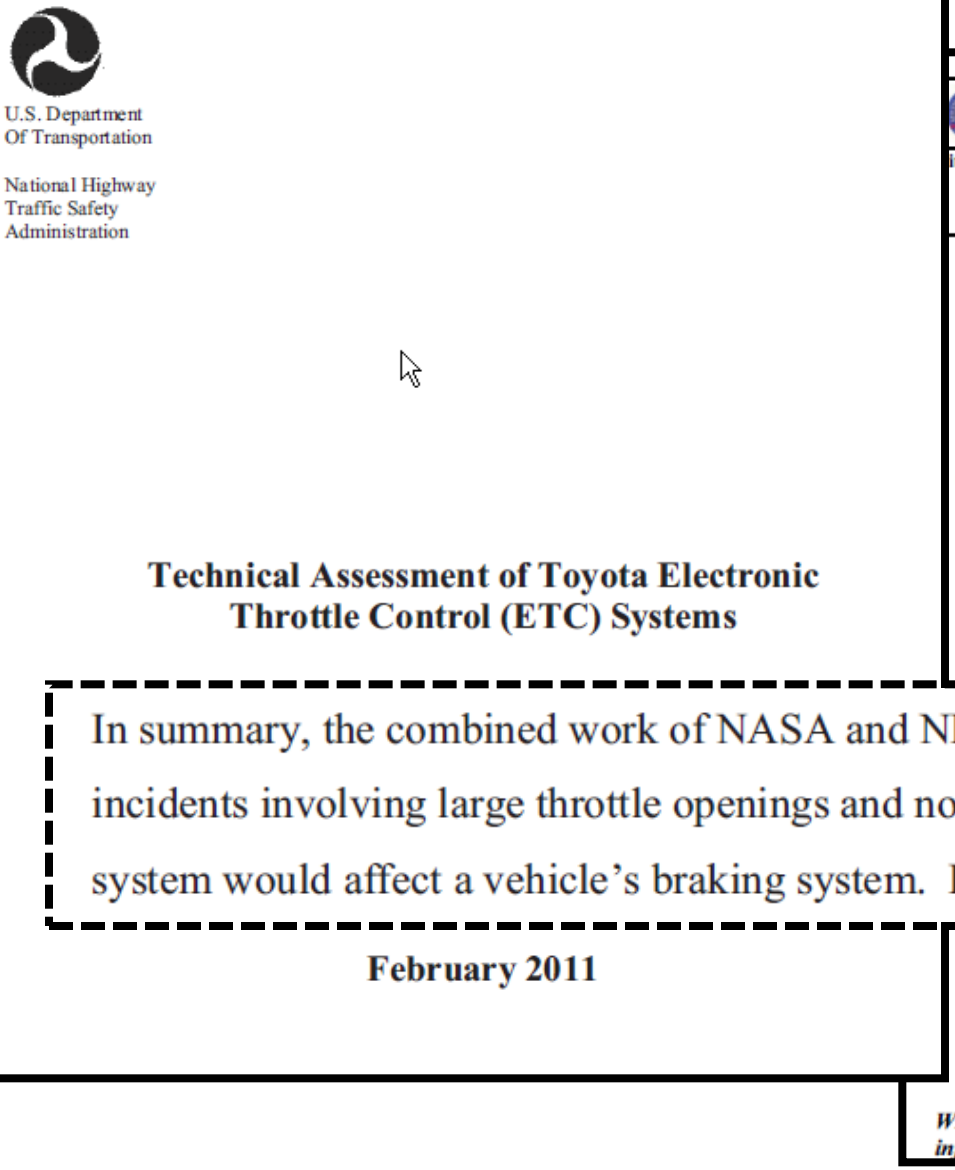
- 実装コードの解析
- ロジックの解析
- モデルベースのテスト
- 実時間性の解析

結果

NASAの解析とテストでは、消費者が報告したような、大きなUAを引き起こすETCの不具合の証拠は見つからなかった。

NASAとNHTSAの調査レポート

SEC
Software Reliability Enhancement Center

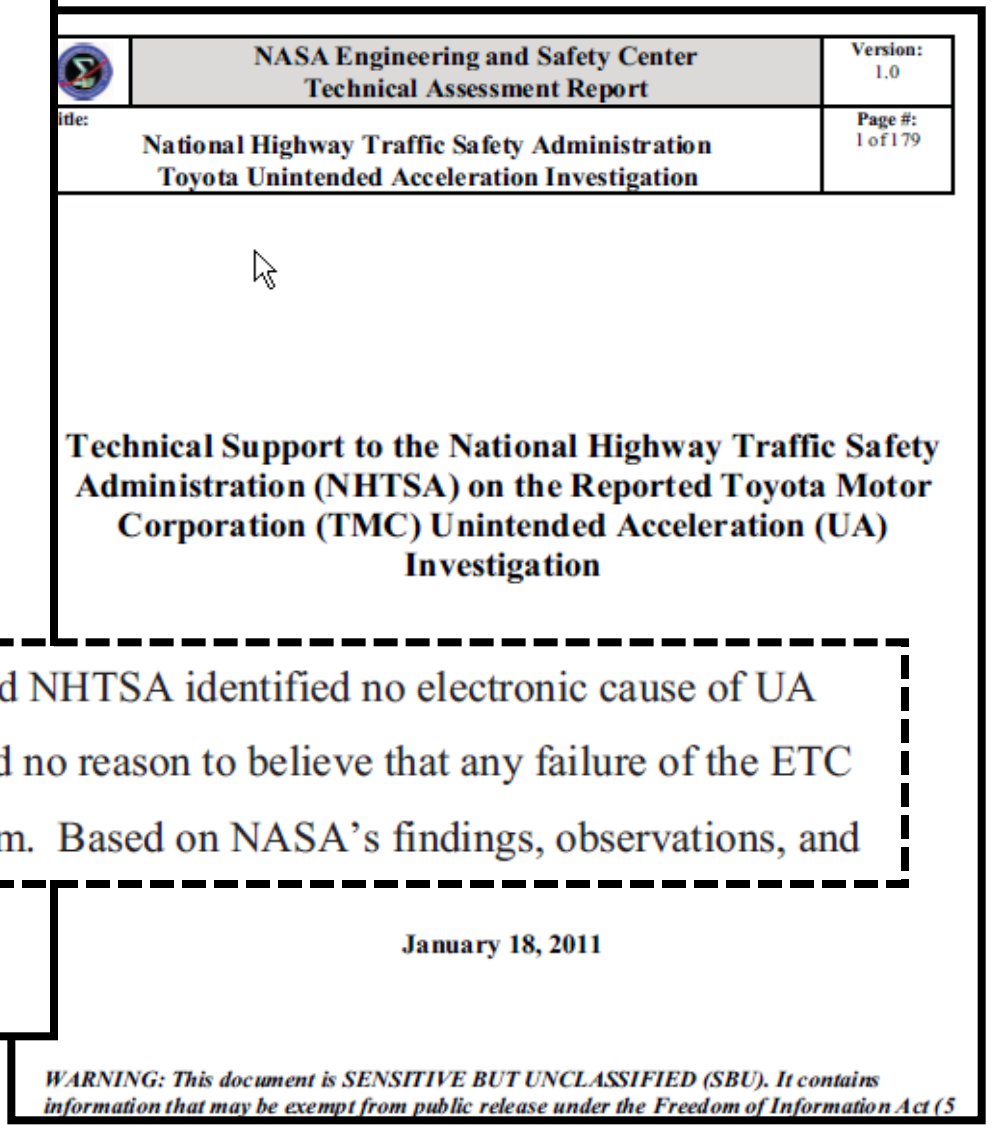


U.S. Department
Of Transportation

National Highway
Traffic Safety
Administration

Technical Assessment of Toyota Electronic Throttle Control (ETC) Systems

February 2011



NASA Engineering and Safety Center Technical Assessment Report	Version: 1.0
itle: National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation	Page #: 1 of 179

Technical Support to the National Highway Traffic Safety Administration (NHTSA) on the Reported Toyota Motor Corporation (TMC) Unintended Acceleration (UA) Investigation

In summary, the combined work of NASA and NHTSA identified no electronic cause of UA incidents involving large throttle openings and no reason to believe that any failure of the ETC system would affect a vehicle's braking system. Based on NASA's findings, observations, and

January 18, 2011

WARNING: This document is SENSITIVE BUT UNCLASSIFIED (SBU). It contains information that may be exempt from public release under the Freedom of Information Act (5

グローバル展開では客観的な評価が重要

SEC Software Reliability Enhancement Center

- これまでの日本企業は、利用者の要望に個々に答えることで高品質というブランド力を築いてきた
  - 実際、日本製のソフトウェアの品質は海外に比べて1桁以上高いとの調査報告もある
- しかしながら、グローバル市場においては客観的・合理的な説明が必要
  - 会計処理における公認会計士による会計監査の必要性と同等

客観的・合理的な説明

- 国際標準（ISO/IEC）等、世界的に合意されている基準類を用いた説明、または、それに準じた説明　→ 規格適合、規格認証 等
- 専門性のある第三者による説明　→ 第三者確認、第三者証明 等
- 公的な機関による説明　→ 公的認証、規制 等

（参考）日米のソフトウェア品質比較

SEC Software Reliability Enhancement Center

（参考）日米のソフトウェア品質の比較

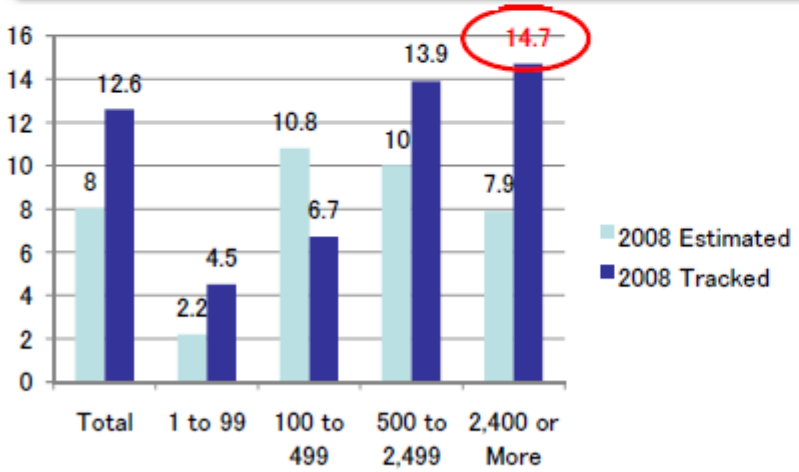
経済産業省 Ministry of Economy, Trade and Industry

比較①： ソフトウェアの不具合数に関する国際比較 → 日本のソフトウェア開発は、他国と比べて不具合が少ないと言われている

	日本	米国	インド	欧州他	計
プロジェクト数	27	31	24	22	104
ソフトウェアの品質 システム導入後1年間に発見された1Kあたりの不具合報告（中央値）	0.020	0.400	0.263	0.225	0.150

出典：CUSUMANO,M.等（IEEE Software Nov./Dec. 2003, pp28-34）

比較②： 情報システムの月間停止時間に関する日米比較 → 日本の方が、10倍以上停止時間が短いと言える（米国14.7時間／月 vs 日本1.32時間／月）



出典：ガートナーリサーチ “Dataquest Insight: Unplanned Downtime Rising for Mission-Critical Applications” (2008年9月分析、10月3日発行)、ガートナーコンサルティング分析

米国のミッションクリティカルなアプリケーションの平均停止時間

選択項目	1件当たりの月間停止時間（時間）（※）	回答件数	月間停止時間合計（時間）
1. 99.999%以上（5分）	0.0072	64	0.461
2. 99.99%以上（50分）	0.0720	64	4.608
3. 99.90%以上（8.6時間）	0.7200	48	34.560
4. 99%以上（86時間）	7.2000	24	172.800
5. 98%以下（175時間）	14.400	4	57.600
合計	1.3200	204	270.029

※1ヶ月の稼働時間を30×24=720時間として停止時間比率をかけたもの

出典：「企業IT行動調査2008（社団法人日本情報システム・ユーザー協会、2008年4月）」のデータを基に計算

日本の従業員が1,000人以上の規模の基幹系システムの稼働実績

13

出典：経産省「高度情報化社会における情報システム・ソフトウェアの信頼性及びセキュリティに関する研究会」中間報告書、2009.5

Copyright © 2013 IPA, All Rights Reserved

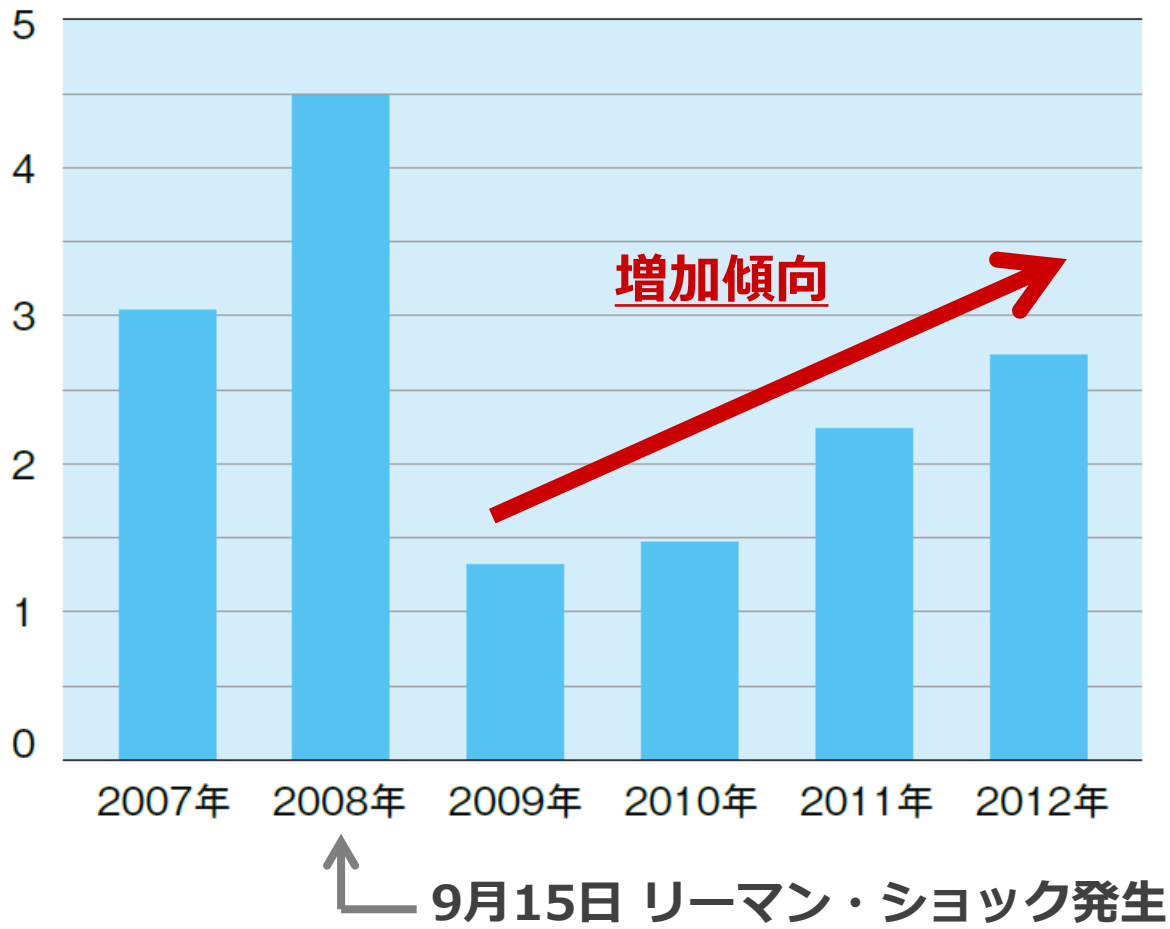
（背景）
複雑化・高度化でソフト起因の障害は増加傾向？

Copyright © 2013 IPA, All Rights Reserved

国内におけるIT障害の発生件数

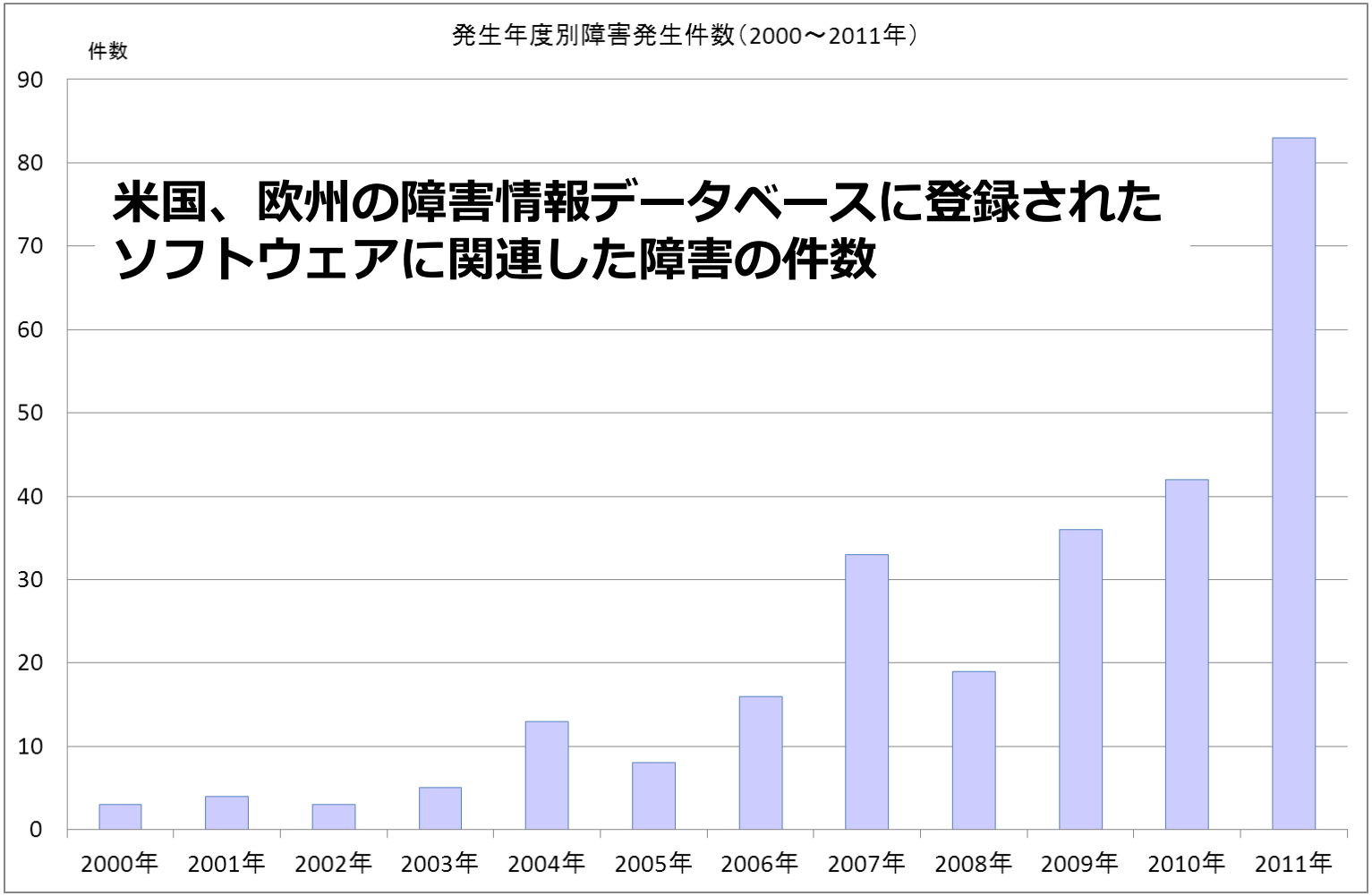
SEC
Software Reliability Enhancement Center

社会経済活動に悪影響を与えたＩＴ障害の発生件数 （月平均、報道ベース）



出典： SEC Journal 第32号 （2013年3月発行）

海外のIT障害の発生件数



米国、欧州の障害情報データベースに登録された
ソフトウェアに関連した障害の件数

※ 出典：IPA/SEC 「海外におけるIT障害の影響及び対応策に関する事例調査」報告書（2013/04）

海外のIT障害事例（ソフトウェア関連）

SEC Software Reliability Enhancement Center

No	国	発生年	タイトル	経済損失額	概要
1	米国	2010	保険請求処理システムのソフトウェア問題による障害	1億1,400万ドル	New York州の保険請求処理システムの不具合により不正請求が検出できず、医療費の過払いが発生。
2	米国	2011	量的投資モデルのソフトウェアバグによる障害	2億1,700万ドル	量的投資モデルのソフトウェアバグが隠蔽されたことにより、約600社の顧客に総額2億ドル超の損害をもたらした。
3	米国	2004	銀行の取引システムのソフトウェアバグとセキュリティによる障害	１億ﾄﾞﾙ	取引処理システムのバグにより数百万口座が影響を被り（復旧に２週間）、さらに同障害を原因とする大規模なメールフィッシング被害が発生。
4	英国	2012	納税システムのソフトウェアバグによる障害	数百万ポンド	納税システムの障害により7百万人の納税者に過払いあるいは支払不足が発生。
5	英国	2011	シェアードサービスシステムの障害	370万ポンド	SAPのソフトウェアシステム障害により、英国Somerset州議会による過払いが発生。
6	米国・カナダ	2003	大規模停電（ITシステム停止）	60億ドル	MSBlastワームが原因とみられるシステム障害と人為的ミスにより、米国、カナダにまたがる大規模な停電が発生。大都市での交通マヒや、航空会社、証券取引所等のシステム停止により、多大な経済損失が発生。
7	米国	2008	鉄道自動発券機の障害	7.4万ドル	鉄道自動券売機のソフトウェアバグにより、一部のチケット購入が無料となった。
8	豪州	2010	航空券予約発券システムの障害	2,000万ドル	航空会社の新システムへの移行時に予約システムに障害が発生し、国内空港の便に遅れが発生。
9	米国	2009	Eコマースの支払いシステムの障害	720万ドル	ネットワークのハードウェア障害により、サービスの停止とパフォーマンスの低下を招き、最悪の障害は１時間継続した。

※ 出典：IPA/SEC 「海外におけるIT障害の影響及び対応策に関する事例調査」報告書（2013/04）より

Copyright © 2013 IPA, All Rights Reserved

複雑化・高度化するシステム（IT融合）

SEC
Software Reliability Enhancement Center

コントロールセンター

地域のエネルギー需給を最適化するコントロールセンター

- 太陽光発電、風力発電、小水力など自然エネルギーを電源として積極的に活用
- 変動の多い自然エネルギーを地域内で有効活用するため、各家庭やオフィスで余った電力を地域内で融通
- 電気バスや電気自動車の位置情報と充電状態を管理することで、これらの自動車を電力インフラとして活用

エネルギーネットワークと一体になった新しい交通インフラ

EVや電気バス同士で情報をやりとりすることにより、
飛躍的な低炭素化と事故や渋滞問題の解決を同時実現

架線レス路面電車

蓄電池を搭載した路面電車
駅での停車時：電池に充電
駅間の移動時：電池で駆動

急速充電ステーション

30分で80%充電

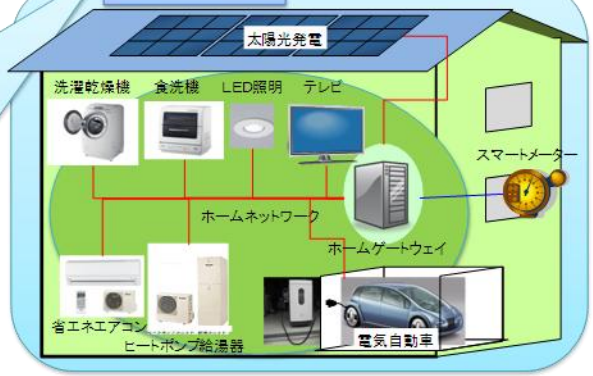
医療／ものづくりなど

・テーラーメード化された医療の提供
・GPSを活用した自動車両誘導システム

EVを電力インフラとして活用

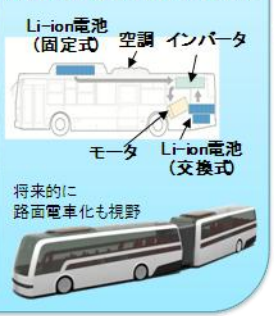
電力不足時：電気自動車→家庭
電力過剰時：家庭→電気自動車

スマートハウス



電気バス（将来は路面電車化）

電池交換式の電気バス。将来的には複数台を連結して路面電車化



センサ等を活用した農業

各種情報を分析し、
最適な生産手段を可能に

（出典）スマートコミュニティ関連システムフォーラム資料、三菱重工資料より経済産業省作成

Copyright © 2013 IPA, All Rights Reserved

IT融合システムでの品質面における課題

SEC Software Reliability Enhancement Center

「つながる」に求められる高度な品質の確保

- 単一企業での構築は難しく、異業種の事業者間での連携が不可欠
- 業種が異なると品質や信頼性に関する規範・基準も異なってくる
- 個々の製品・サービスが高品質でもシステム全体の品質は必ずしも保証されない
- 新しい技術領域であり、業界をまたがった仕様整備・標準化が必要

市場の拡大には利用者の理解と安心感が不可欠

- 便利な製品やサービスは使いたいが、新しい技術には不安がある
- 多くの事業者が関わるシステムでだれが責任を持っているのか不明
- 利用形態の多様化とシステムの複雑化によるギャップの拡大
- **利用者に対する品質説明**がこれまで以上に求められる

Copyright © 2013 IPA, All Rights Reserved

IT融合領域におけるソフトウェアの重要性

SEC Software Reliability Enhancement Center

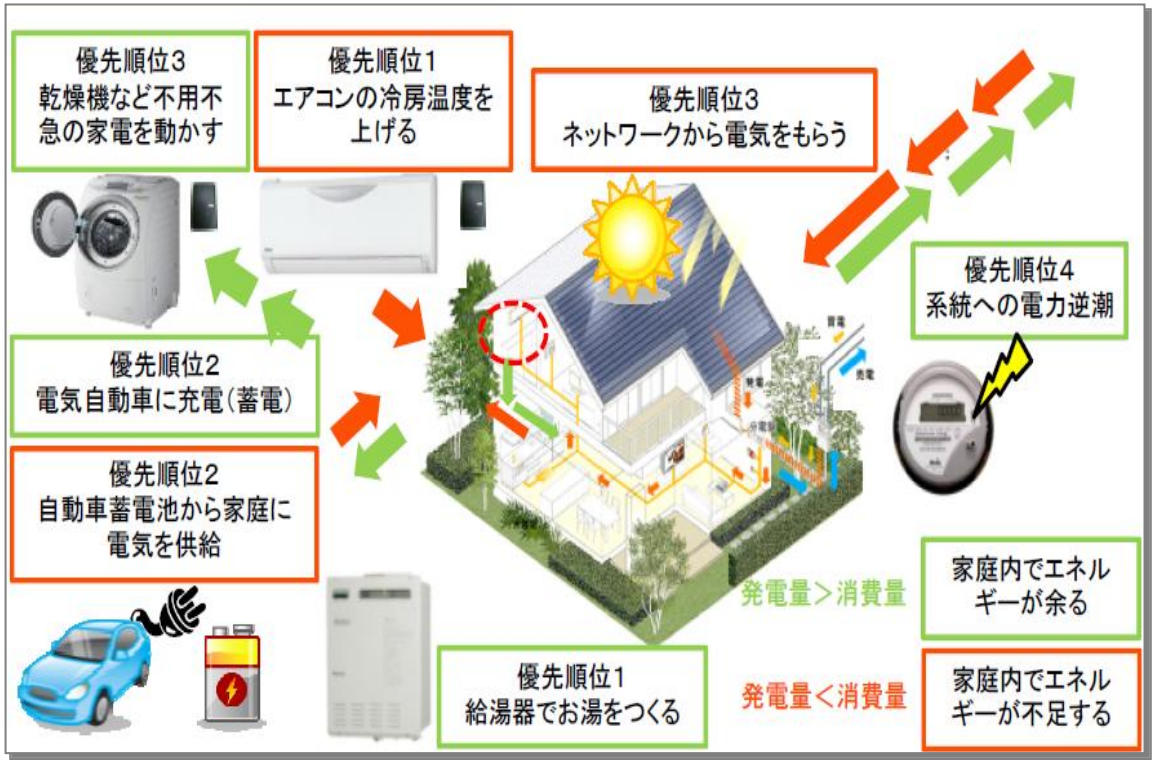
■ IT融合システムの特徴：

- 構成機器およびサブシステムが自律的に動作
- 全体として連携・協調動作するシステム
- 複雑な機能の実現にソフトウェアの役割が増大

（出典） 経済産業省資料より

例）スマートハウスにおける主な制御機能

- 各接続機器からのデータ収集、蓄積、分析
- 系統電力一定制御、ピークカット
- 機器への動作指示（バッテリ充放電制御、家電省エネ運転、EV/PHV制御）
- 停電時対応、障害対応
- 発電量、消費量、各機器の運転状態等を居住者へモニタ表示
- セキュリティ



Copyright © 2013 IPA, All Rights Reserved

障害事例（海外）

■スマートメーター障害事例（１）

2006年～、2009年訴訟、2010年に障害調査報告書(約700頁）公開。
北米（カリフォルニア州、テキサス州）、パシフィック・ガス&エレクトリック(PG&E)
「 トータル45,000件のスマートメーターが正常動作せず！」

No.	障害概要	障害の原因	件数	被害状況	原因分類
1	ソフトウェアのプロセス異常に起因する頻繁なリブート。	ソフトウェア障害	12,763件	検針データが失われ、料金過小請求につながった。	SW
2	スマートメータ種別(事業者用、住宅用）を間違ってソフトをインストール。	出荷時もしくは、設置作業者のミス	2,900件	検針データが不正値となり、電力会社側のシステムにも影響 を与えた。メーター交換。	SW 運用

■スマートメーター障害事例（２）

2010年5月　北米（ペンシルバニア州）、サンディエゴガス&エレクトリック（SDG&E）

No.	障害概要	障害の原因	件数	被害状況	原因
3	スマートメータのソフトウェア更新中に停電し、更新できず。	システム検討不足	30,000件	通信できなくなった。メーター交換。	SW 保守

※ 出典：IPA/SEC 「海外におけるIT障害の影響及び対応策に関する事例調査」報告書（2013/04）より

Copyright © 2013 IPA, All Rights Reserved

（背景）
利用者にもITリテラシーが求められるが…

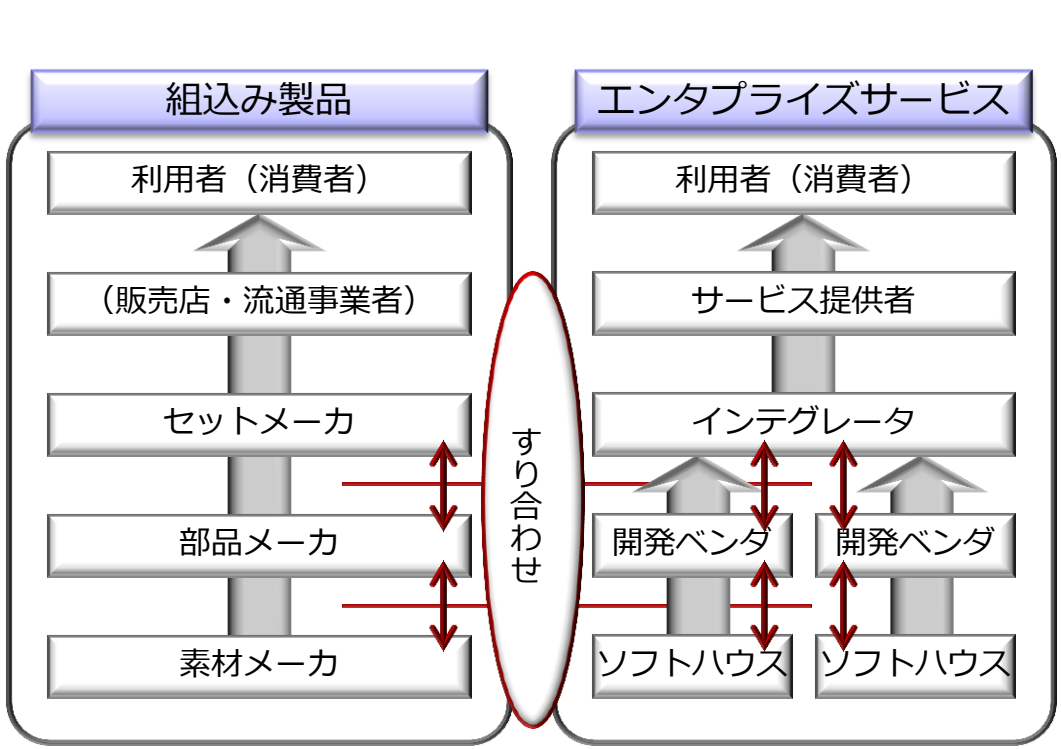
Copyright © 2013 IPA, All Rights Reserved

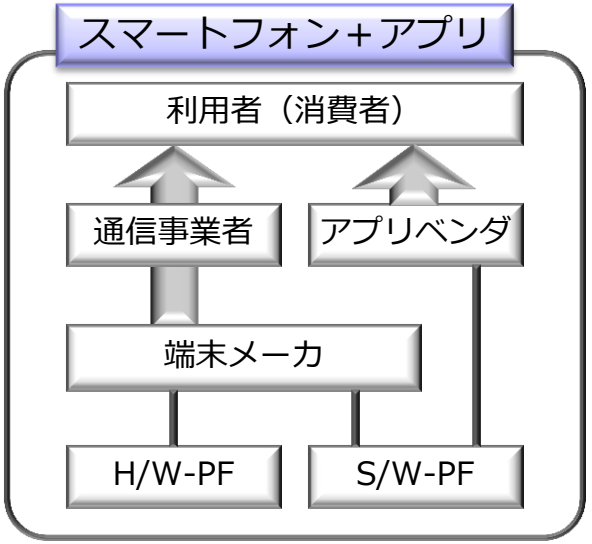
ものづくりと流通の変化・多様化

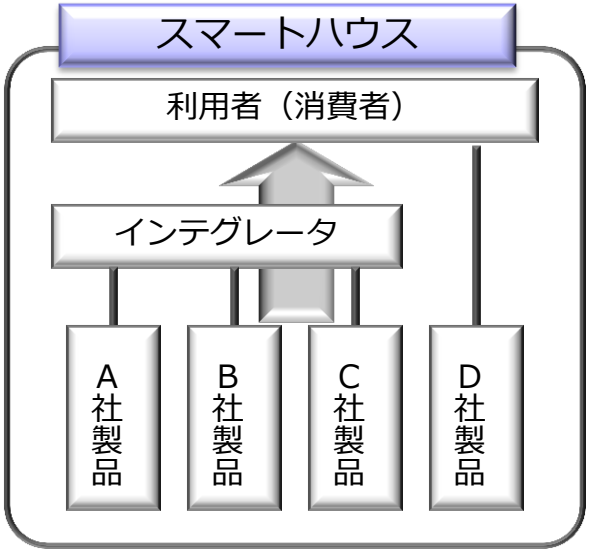
SEC
Software Reliability Enhancement Center

■ **ユーザ側でのインテグレーション**

従来の製品・システムは、メーカやインテグレータにより最終製品・システムが品質高く作り込まれてきた。一方、最近のスマートフォン＋アプリや、スマートハウスを構成する機器は、様々な出所の製品等は組み合わされ、随時入れ替えられることがあるため、全体の信頼性の担保が難しくなっている。







Copyright © 2013 IPA, All Rights Reserved

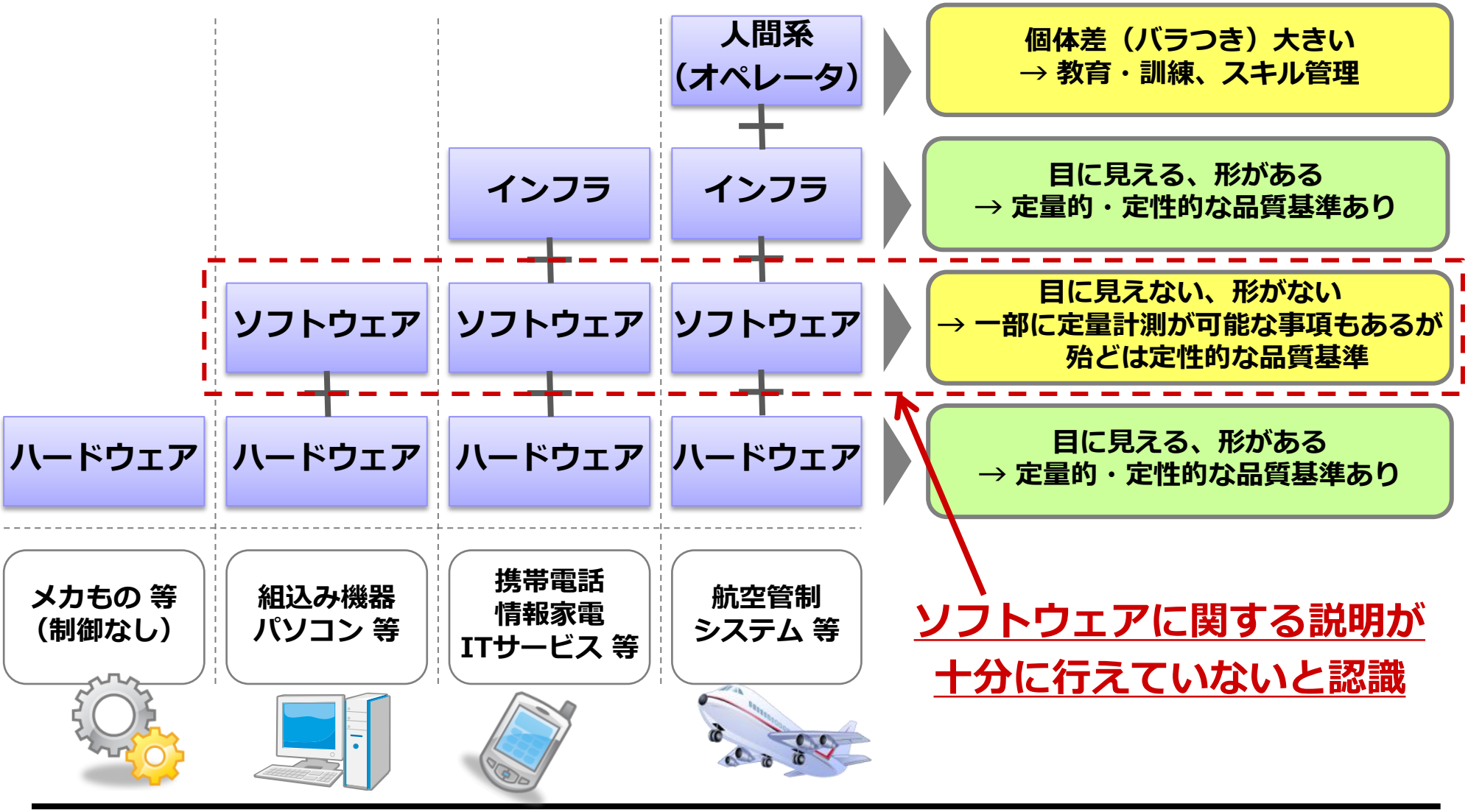
利用者が製品等を組み合わせて使用

SEC Software Reliability Enhancement Center

- 従来型の製品・サービス、システム
  - 垂直統合（すり合わせ）型の開発で品質を保証
- 新しい製品（分野）の登場・拡大

  これからは
  - 利用者自らが、（供給者の異なる）製品・サービスやシステムを選択し、組み合わせて使用
    - 例：スマートフォン＋アプリ、HEMS＋家電機器 等
    - 利用者の手元で品質の組み合わせ問題が発生
    - 事前に全ての組み合わせを想定・検証し、品質保証をすることは不可能
- しかし、技術的に詳細な説明は（利用者には難しくて）わからない、理解できない

製品・サービス、システムの構成要素



「背景」のまとめ

SEC
Software Reliability Enhancement Center

① グローバル市場においては当事者企業の主張だけでは不十分で、第三者による客観的な評価の裏付けが必要

② IT融合システムの市場の拡大には利用者の理解と安心感が不可欠であり、利用者に対する品質説明が重要

③ 利用者自らが、製品・サービスやシステムを選択し、組み合わせて使用する時代。しかし、技術的に詳細な説明は利用者には困難

第三者が品質を客観的に確認して利用者にわかりやすく示す仕組みが求められている

Copyright © 2013 IPA, All Rights Reserved

（ソフトウェア品質説明とは？）
品質説明の4つのポイント

Copyright © 2013 IPA, All Rights Reserved

「品質説明」と「品質説明力」

SEC
Software Reliability Enhancement Center

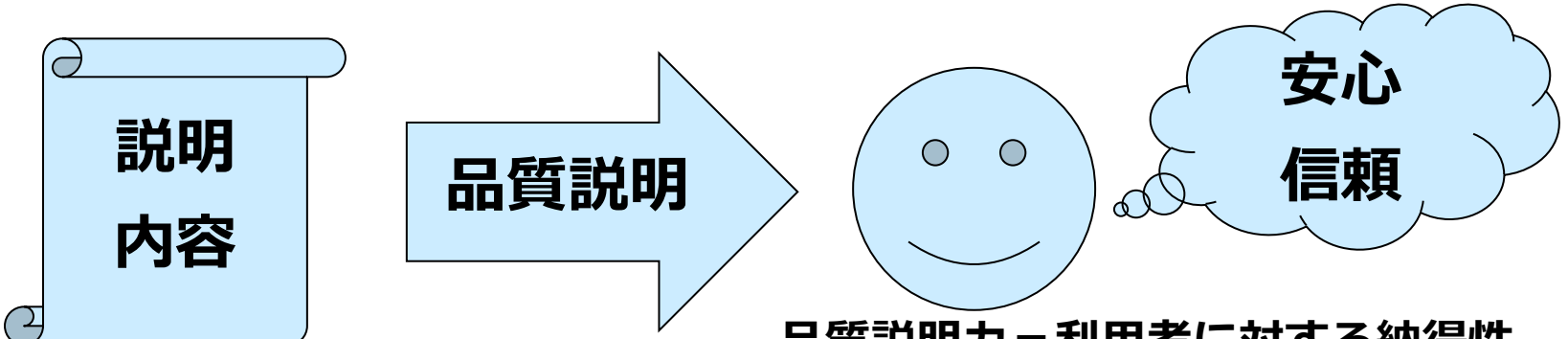
品質説明

利用者が品質を確認し判断できるように製品・システムの供給者が利用者に対して説明をすること

品質説明力

品質説明を行う力（能力）、品質説明による効果

供給者が持ち合わせている力（能力）やそれによる効果ではなく説明そのものの力（能力）やその効果を指す



品質説明力＝利用者に対する納得性、利用者に対する効果

Copyright © 2013 IPA, All Rights Reserved

品質説明の要素

SEC
Software Reliability Enhancement Center

ソフトウェアが重要な役割を果たす製品・システムにおいて以下の事項を根拠や事実に基づいて説明すること

- 想定する利用者、利用目的、利用状況、制約事項
- 利用する上で必要なソフトウェアの品質とその目標
- 品質目標を達成するための設計・実装・運用および保守
- 品質目標を達成したことの検証・監査

＜注意＞
ソフトウェアに関する説明を行えば、その製品・システムの品質の説明になるということを意図するものではない

Copyright © 2013 IPA, All Rights Reserved

品質説明（良い例、悪い例）

SEC
Software Reliability Enhancement Center

✓ 良い例

明確な
品質目標

品質目標

相互参照可能

◆どんな設計をしたら
品質目標を達成できるか
◆どんなテストをしたら
目標達成を確認できるか

品質目標を
達成するための
ロジック

相互参照可能

テスト
結果

設計
書

管理され
たプログ
ラム

証拠

✓ 悪い例

考慮漏れ

不明瞭な
品質目標

明確な
品質目標

？？？？？

テスト
結果

設計
書

プログラ
ム

Copyright © 2013 IPA, All Rights Reserved

品質説明のための手法例

SEC
Software Reliability Enhancement Center

アシュアランスケース

システムの安全性、ディペンダビリティなどを、エビデンスをもとに議論するための文書

- **アシュアランス（Assurance:保証）、ケース（Case:論拠）**
- **1988年の北海油田事故（167名死亡）などを契機に、欧米で規格認証の際に義務付けられるまでに普及**
  - ✓ **手順やチェックリスト等だけではなく、なぜ安全性が保たれるか、明示された議論で、エビデンスをもとに保証する**
  - ✓ **導入により北海油田における事故が減少**
- **安全性を議論する場合はセーフティケース、ディペンダビリティを議論する場合はディペンダビリティケースと呼ばれる（歴史的にはセーフティケースが最初でそれが一般化された）**

参考：松野、高井、山本「D-Case入門 ～ディペンダビリティ・ケースを書いてみよう！～」」

表記法例：ＧＳＮ（Goal Structuring Notation）

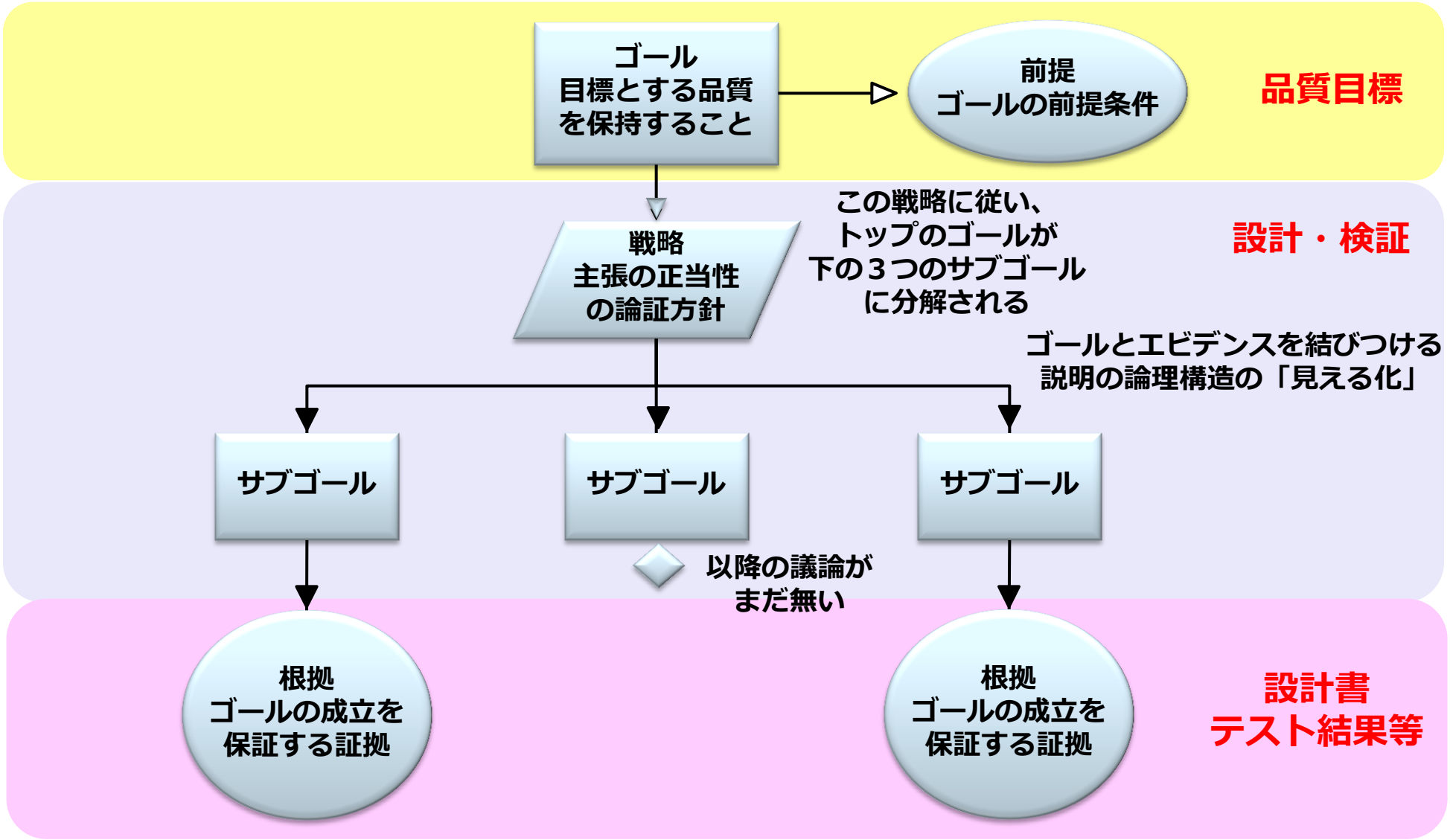
SEC Software Reliability Enhancement Center

● 保証のための構造化された議論の記述法(T.Kellyらにより開発)
- GSN Community Standard Ver.1.0

	ゴール（Goal）	保証したいこと、命題（例：システムは安全である） ゴールはさらに詳細なゴール（サブゴール）に分解される
	前提（Context）	システムの状態、環境などゴールを議論するときの前提等 （例：リスク分析の結果得られたハザードのリスト）
	戦略（Strategy）	ゴールをサブゴールに分けるときの考え方 （例：個別の障害ごとに議論する）
	根拠 （Evidence/Solution）	ゴールが成り立つことを最終的の保証するもの （例：テスト結果、運用事例など）

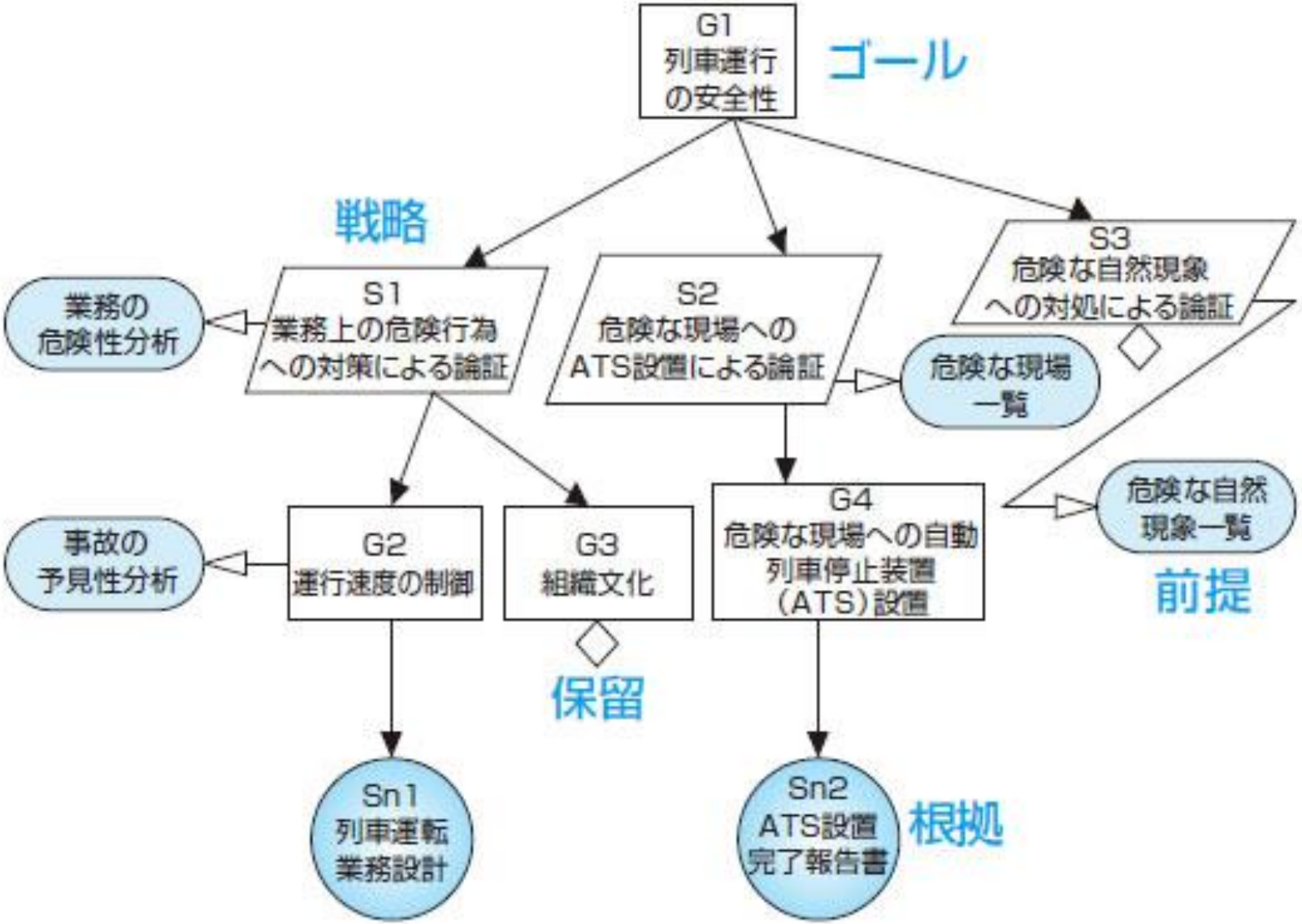
参考：松野、高井、山本「D-Case入門 ～ディペンダビリティ・ケースを書いてみよう！～」」

品質説明の表記イメージ



Copyright © 2013 IPA, All Rights Reserved

記 述 例



出典：名古屋大学 山本修一郎教授「D-Case実証評価研究会の狙い」

Copyright © 2013 IPA, All Rights Reserved

（ソフトウェア品質説明とは？）
説明力強化の3つの視点

Copyright © 2013 IPA, All Rights Reserved

説明力強化の３つの視点

SEC
Software Reliability Enhancement Center

技術的側面

供給者が製品・システムを開発・運用する過程において、要求される品質を確保するための開発・運用技術
　ex. モデルベース開発、形式手法、トレーサビリティ、検証技術

管理的側面

製品・システムのライフサイクル全般にわたる組織的な品質マネジメント

制度的側面

供給者による品質説明の適切性を第三者が確認し、利用者に提供する仕組み（制度）の構築
公正かつ専門的な観点での評価により利用者の安心感を醸成

技術的側面の例

Copyright © 2013 IPA, All Rights Reserved

モデルベース開発のメリット

SEC
Software Reliability Enhancement Center

■ 正確な設計が可能になる

書き方・読み方が定まった記述方法を用いることにより、記述もれ、曖昧さ、重複などの少ない、より正確な設計を行えるようになる。それに伴い、設計の正しさの確認もより厳密に行えるようになる。

■ 設計が見えるようになり、レビュー効率アップ

ソフトウェアの設計がより把握しやすくなり、レビュー効率がアップする。また、品質管理のベースとして様々な計測を行うこともできるようになる。

■ コミュニケーションが円滑になる

正確かつ捉えやすい設計書を記述することにより、開発に関わる様々な人の間でのコミュニケーションがスムースに行われるようになる。

■ シミュレーションや検証をツール化できる

従来設計書の確認は人手でレビューするしかなかったが、モデル化を行うことにより、ツールによるシミュレーションやチェック機能を活用する道が開ける。

■ 標準化が促進され再利用が容易になる

標準記法を用いることにより、設計書の標準化が促進され、再利用が容易になる。

（出典） SECBOOKS　組込みソフトウェア開発における品質向上の勧め【設計モデリング編】

Copyright © 2013 IPA, All Rights Reserved

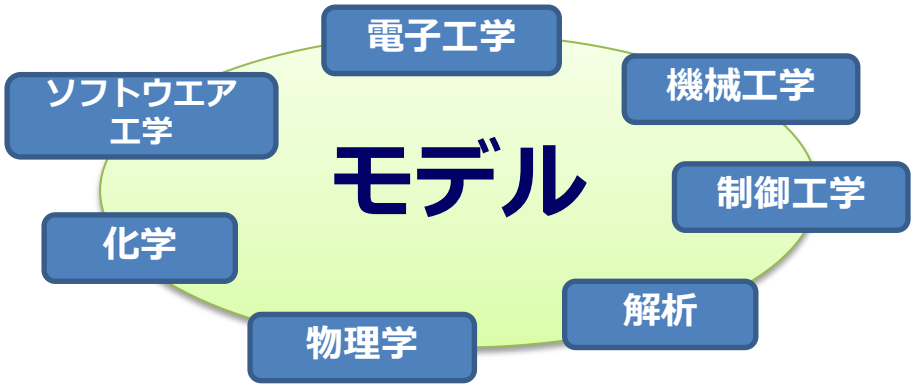
MBSEとは（システムズエンジニアリング技術）

SEC Software Reliability Enhancement Center

- エンジニアリング領域の拡大と大規模複雑化
  - → 開発関係者の多様化
  - → ドキュメントの増加

- 効率的な記述言語とコミュニケーション方法が必要
  - → モデルの導入へ
    MBSE（Model Based Systems Engineering）
    によるシステム開発が効果的

- MBSEとは、モデルを活用したシステムズエンジニアリング
  - 様々な分野をモデルで橋渡し
  - モデルによる効率的な記述
    - 代表的なモデリング言語がSysML



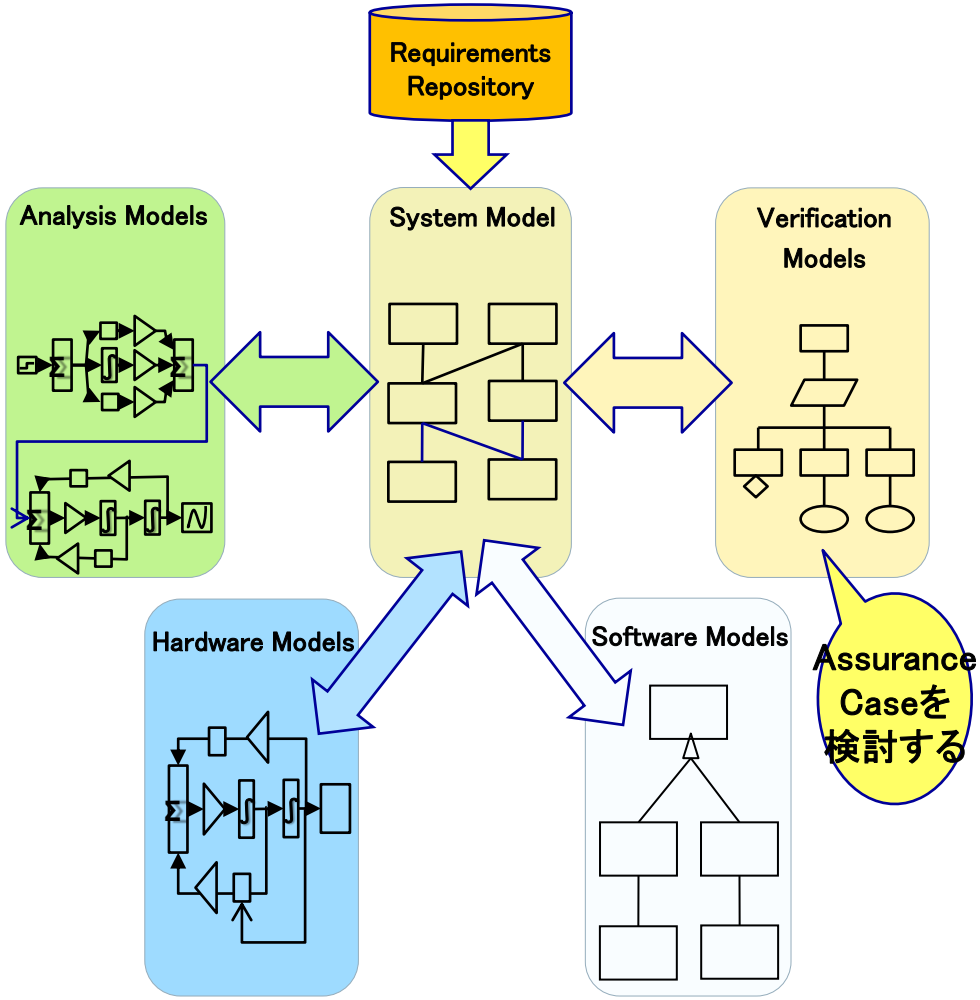
Copyright © 2013 IPA, All Rights Reserved

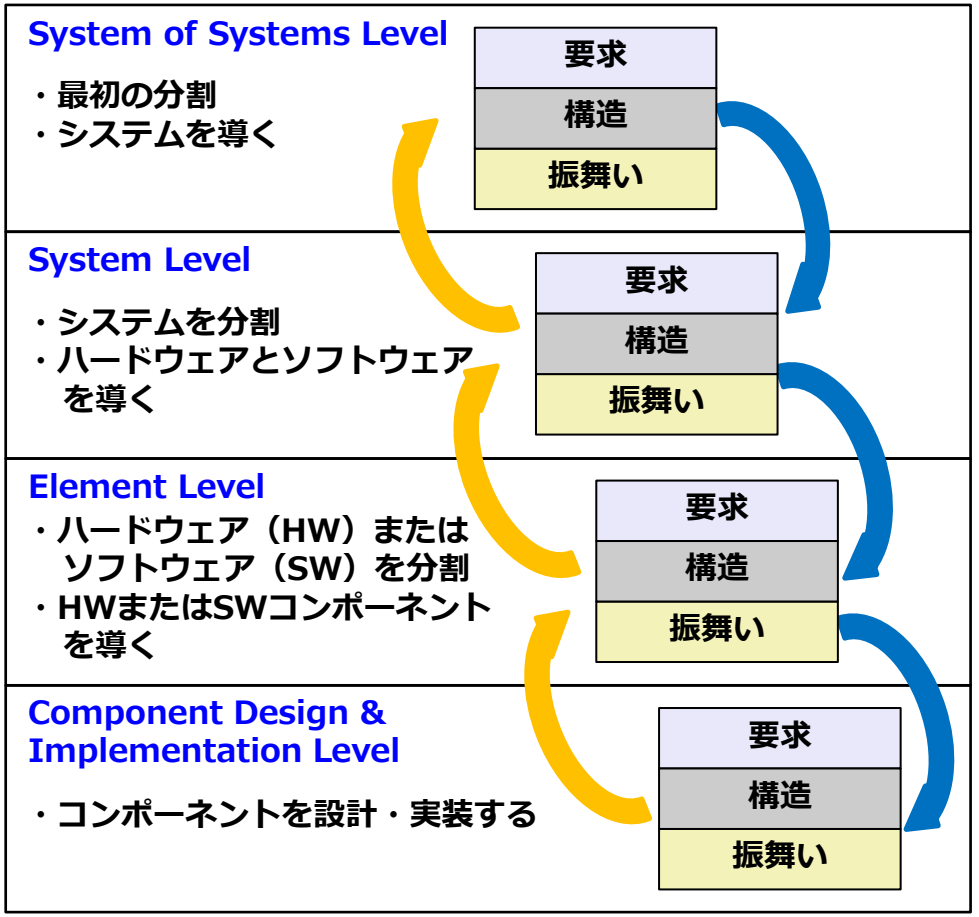
MBSEの基本構造とスコープ

SEC
Software Reliability Enhancement Center

システムを適切にハードウェアとソフトウェアに分割できるため、QCDSE(品質、コスト、納期、安全性、環境)等のバランスをとることができる

階層的にシステムを扱うことができる





Copyright © 2013 IPA, All Rights Reserved

高信頼システム開発技法としての形式手法

SEC Software Reliability Enhancement Center

- 「形式手法」はシステム開発において
  ・仕様の曖昧さを無くす
  ・設計のミスを防ぐ
  ・実装の間違いを見つけ出す
  といった利点があり、鉄道、航空、原発等重要インフラ等のシステム開発において、高信頼性を担保するために有効な技術

- 1990年代後半から欧州では、安心・安全な生活基盤を整備するため、形式手法を適用したシステム構築が進展。この結果、重要インフラ等、高信頼性を要求される実システムの開発プロジェクトで形式手法の適用が日本に比べ先行した。

- 国際標準において、形式手法の適用は一般的な機械を対象とした機能安全規格等で推奨されている。

Copyright © 2013 IPA, All Rights Reserved

形式手法適用(実用化)海外事例

SEC Software Reliability Enhancement Center

形式手法が進む欧州においては、いまだ限定的だが重要インフラを中心に適用（実用化）が進んでいる
（情報系よりも組込み系が主、企業情報システムでは、セキュリティやネットワーク関連が中心）

形式手法の情報システム系重要インフラへの適用（実用化）の概要

重要インフラ領域	適用国	システム名	適用企業・機関（システムベンダーなど）	適用開発工程	適用形式手法・ツール
情報通信	独	ネットワークプロトコル仕様	Lucent Technologies Network Systems GmbH	設計	ADeVA(言語入力、VHDL変換)、GateProp(モデル検査)、VHDL
	伊	船舶向け通信システム	Selex Communications、University of L'Aquila	設計・テスト	CHARMY(アーキテクチャ・時相制約記述、SPINへの変換)、DEPCOL(性質抽出)
金融	インド	生命保険関連情報システム	The Research Development and Design Centre	要求分析	Requirements Modeling Tool (図からSAL形式への変換・解析)
航空	英	航空機エンジン制御システム	University of York	設計	SCANN、SLANN(独自の設計手法)、HAZOP(リスク分析手法)
鉄道	仏	鉄道制御システム、駅乗車ホーム防御ドア制御システム	ClearSy、Siemens Transportation Systems	設計、実装	B、Atelier B、EDith B、Bertille(仕様詳細化支援ツール)、Brama、LADDER(言語)
電力・ガス・水道	独・韓国	原子力発電所制御システム	Institut fuer Sicherheitstechnologie、Korea Atomic Energy Research Institute	設計	N/A
政府・行政・医療ほかその他 注）組込み系を一部含む	独	セキュリティ(医療情報システムアクセス制御、スマートカード等)	Siemens Corporate Technology	設計	Isabelle(定理証明)、モデル検査(独自)、Interacting State machines(独自のオートマトンモデル)
	仏	マイクロカーネル(L4OS)	STMicroelectronics、ClearSy	テスト	Event B、Brama

出所：「高信頼性ソフトウエア構築技術に関する動向調査」（2008年10月、独立行政法人情報処理推進機構、情報源は05年以降の国際会議等に発表されている論文や報告書等の文献）ほか

実務家のための形式手法シリーズ

SEC Software Reliability Enhancement Center

「厳密な仕様記述を志すための形式手法入門 第二版」

とかく形式手法は難しいという開発現場の認識を変えるべく、現場のソフトウェア開発従事者が特に上流工程で苦労している部分への効果を理解できるように、形式手法の現場導入で得られた実践的な知見を反映した教材

「対象を如何にモデル化するか？」

上記教材の「実践法:モデル化の手順と事例」、「実践法:モデル化の課題例」では形式手法を活用する具体的手順と課題を説明しており、その部分の副読本

「厳密な仕様記述入門」

開発ライフサイクルの上流における仕様書についての厳密な定義及び記述に対する入門書。この入門書は、形式手法をベースとして記述しているが、日本語による仕様書記述においても役立つ内容となっている。

Copyright © 2013 IPA, All Rights Reserved

「ソフトウェア品質説明とは？」のまとめ

SEC Software Reliability Enhancement Center

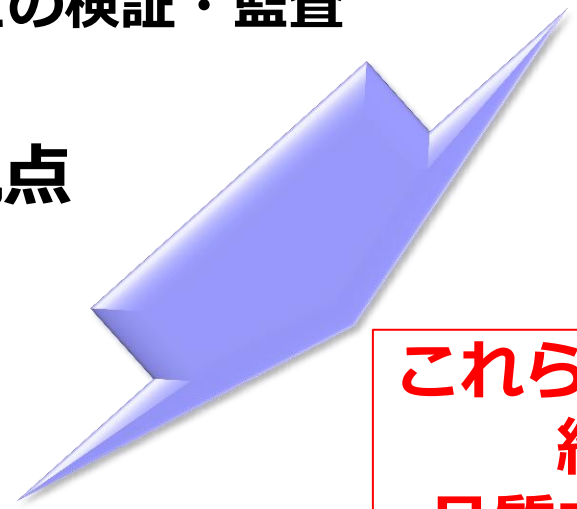
■ 品質説明の４つのポイント

ソフトウェアが重要な役割を果たす製品・システムにおいて
以下の事項を根拠や事実に基づいて説明すること

- 想定する利用者、利用目的、利用状況、制約事項
- 利用する上で必要なソフトウェアの品質とその目標
- 品質目標を達成するための設計・実装・運用および保守
- 品質目標を達成したことの検証・監査

■ 説明力強化の３つの視点

- 技術的側面
- 管理的側面
- 制度的側面



**これらの取組みにより、
結果として、
品質向上も期待できる**

（ソフトウェア品質説明のための制度ガイドライン）
目的・位置づけ

Copyright © 2013 IPA, All Rights Reserved

制度ガイドラインの名称

SEC
Software Reliability Enhancement Center

製品・システムにおけるソフトウェアの信頼性・安全性等に関する品質説明力強化のための制度構築ガイドライン

【通称】 「ソフトウェア品質説明のための制度ガイドライン」

【策定の背景】

供給者に求められるもの

- **高度化・複雑化する製品・システムの品質確保に努めること**
- **製品・システムの品質に関して、利用者に十分な説明を行う責任**

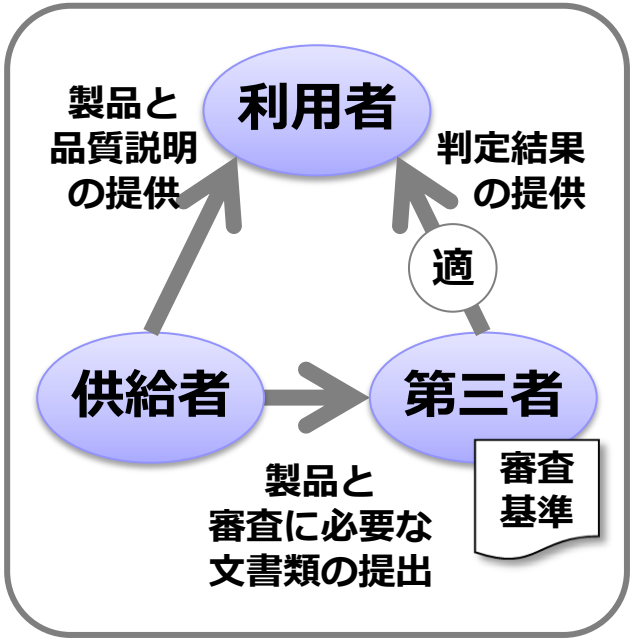
利用者に求められるもの

- **品質に関する情報収集とその理解**

制度ガイドラインの目的

ソフトウェアが重要な機能の実現に関わる製品・システムにおけるソフトウェアの信頼性や安全性等に関する品質について、供給者が利用者に示す説明が適切であることを、第三者が基準に照らして確認し、第三者並びに供給者がその結果を利用者に分かりやすく提供する

上記制度を構築する際の指針を示すことが目的である

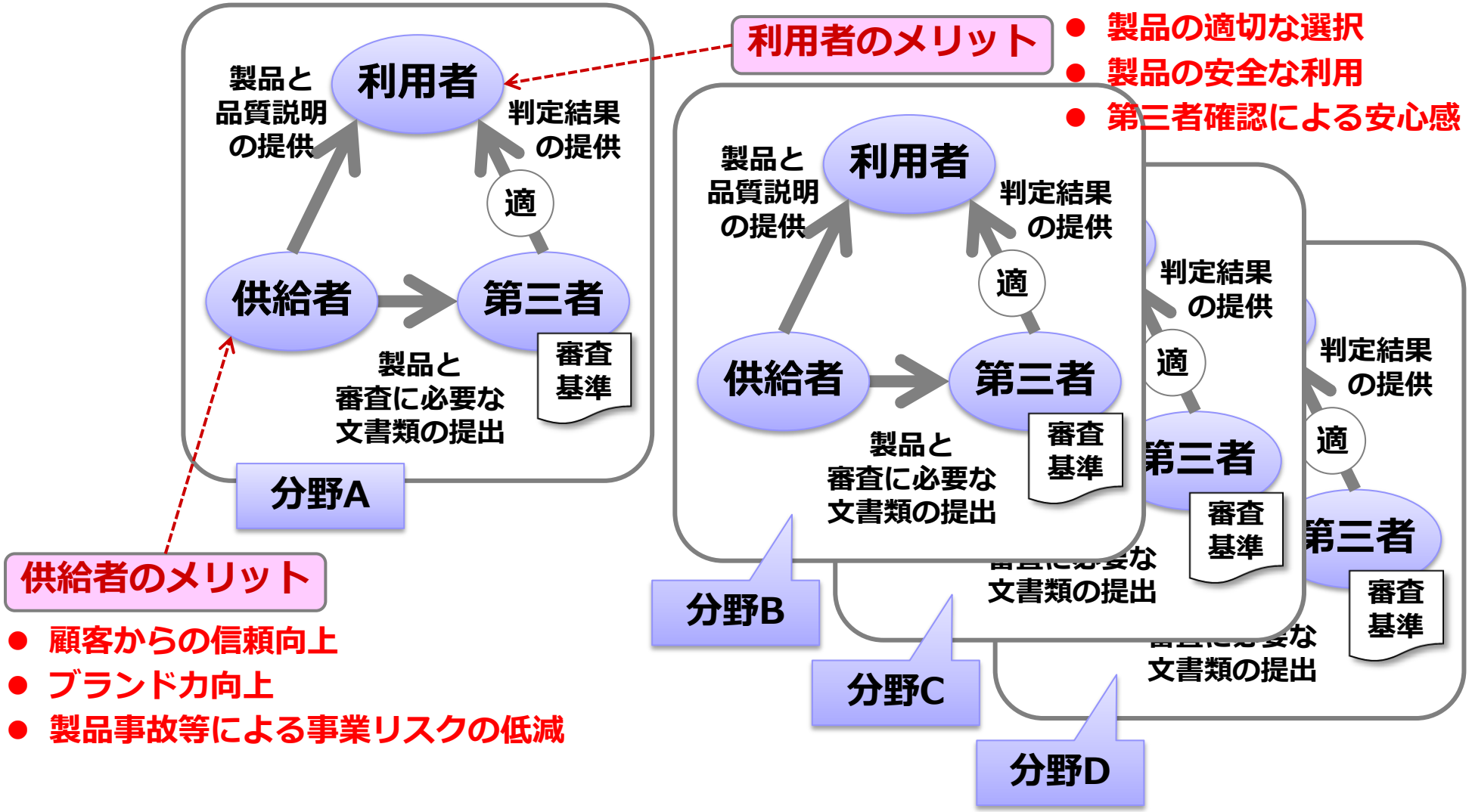


Copyright © 2013 IPA, All Rights Reserved

制度ガイドラインが想定する制度の枠組み

SEC Software Reliability Enhancement Center

製品・システムの分野毎に制度ガイドラインに基づく枠組みが構築される



制度は誰が作るのか？

SEC Software Reliability Enhancement Center

- 制度を構築するかは、製品・システム分野や業界の置かれている状況（規制の有無や国際標準の整備状況等）を踏まえて、**業界団体等が総合的に判断**
- 本ガイドラインの**適用は任意**

以下のニーズがある分野・業界を想定

- 安全・安心につながる公正な情報提供により利用者の信頼を確保したい
- 品質の良い製品を流通させる仕組みを整備したい
- 国際標準や規制がない分野において客観性のある品質説明の基準を整備したい
- 障害発生時に品質に対する説明責任を果たせるようにしたい

Copyright © 2013 IPA, All Rights Reserved

制度ガイドラインが想定する対象分野

SEC Software Reliability Enhancement Center

- 想定している分野
  - まだ、規格が策定されていない、規格の策定よりも技術の進歩が速い分野
  - 複数の製品・システム分野が混在する分野
  - 出荷・リリース段階で利用品質が確定できない分野

- （現時点では）想定していない分野
  - 規格対応、規格認証、法令等に基づく規制等が既にある分野
  - 諸外国との国際的な整合が既に図られている分野

Copyright © 2013 IPA, All Rights Reserved

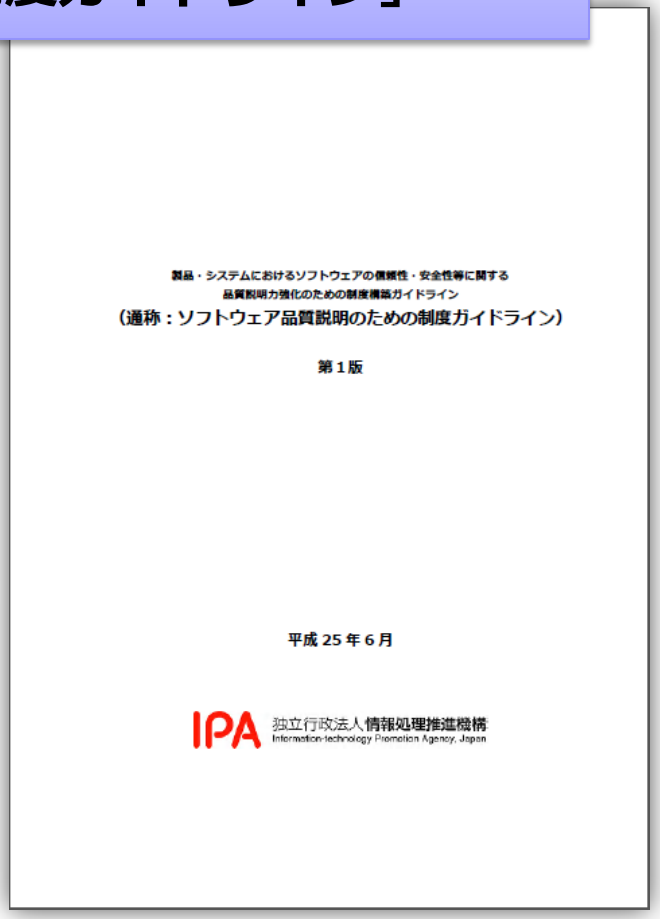
（ソフトウェア品質説明のための制度ガイドライン）
制度ガイドラインの概要

Copyright © 2013 IPA, All Rights Reserved

制度ガイドラインの特徴

SEC
Software Reliability Enhancement Center

製品・システムにおけるソフトウェアの信頼性・安全性等に関する品質説明力強化のための制度構築ガイドライン
【通称】 「ソフトウェア品質説明のための制度ガイドライン」



- **対象**
  - 利用者への品質説明を目的とした制度構築に関心を持つ組織・団体 等
  - 製品・システムの分野毎に個別に適用
- **特徴**
  - 公正性の確保
    - 製品やシステムを確認する第三者と供給者の独立性の確保
    - 制度に関与していない外部者による制度のレビューの実施等
  - 整合性の確保
    - 製品・システムの分野に依存しない要求事項
    - 分野毎に異なる品質要求や技術に対応した審査基準策定の考え方　等

Copyright © 2013 IPA, All Rights Reserved

合理的な仕組みの構築（１）

SEC Software Reliability Enhancement Center

■既存の認証結果の利用

審査基準の基礎となる基準は、次の検討順序による

- 一般に認められた標準（ISO、IECやJIS等）に依拠すること。
  この場合、その標準への適合確認を行うことができる認証機関がある場合は、**その認証結果の確認をもって審査基準の当該部分の審査を行ったこととすることができる。**
- 標準に依拠しない基準を策定する場合は、公正性が説明できること。

合理的な仕組みの構築（２）

SEC Software Reliability Enhancement Center

■利用者等に与える影響に応じた審査

- 製品・システムの不具合や誤使用等によるリスクを評価して、利用者の健康等に及ぼし得る負の影響（人の死亡、負傷等）、財産や社会に及ぼし得る負の影響（経済的な損失等）等を考慮して影響度を段階的に設定することができる（設定されたものを影響レベルという）。
- **影響レベルに応じた審査を実施することにより、利用者にも供給者にも経済的に合理性のある制度の構築ができる。**

利用者等への負の影響

影響レベル	影響の範囲・程度
4	• 当該利用者ならびに当該利用者以外への重大な影響 • 利用者ならびに利用者以外への広範囲で重大な影響
3	• 当該利用者への重大な影響に加え、当該利用者以外への軽微な影響
2	• 当該利用者に限定された重大な影響
1	• 当該利用者に限定された軽微な影響
0	• 影響はない／ほとんど影響はない

財産や社会等への負の影響

影響レベル	影響の範囲・程度
4	• 産業への広範囲な影響
3	• 当該産業に限定された影響 • 当該企業以外の同一・類似産業のへの影響
2	• 当該企業に限定された影響 • 当該製品以外の他事業への影響
1	• 当該製品・サービス事業に限定された影響
0	• 影響はない／ほとんど影響はない

製品の影響レベルは上記２つの観点でレベルを判定し、高いほうのレベルとする

影響レベル設定の参考例

制度ガイドラインの構成

SEC Software Reliability Enhancement Center

はじめに
1. 用語　用語の定義
2. 制度の基本的な考え方　ソフトウェア品質説明力と制度の考え方
3. 個別制度の構築　制度責任主体、制度構成要素の役割や審査基準に関する解説
4. 個別制度に対する要求事項　基本事項、制度責任主体、制度規程の記載事項
5. 本ガイドラインへの準拠表示　個別制度の準拠性の表示方法等
本ガイドラインについての問合せ先　IPAの問合せ窓口等
付録
- 制度構成要素に対する要求事項の例
- 審査機関(審査をする組織)に対する要求事項の例
- 技術的な検証機関(技術的検証をする組織)に対する要求事項の例
- 制度構成要素に属す要員に対する要求事項の例
- 制度構成要素外の審査専門家を確保する場合の審査専門家に対する要求事項の例

Copyright © 2013 IPA, All Rights Reserved

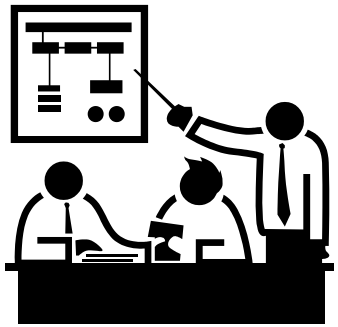
制度責任主体と制度構成要素

SEC
Software Reliability Enhancement Center

- **制度責任主体・・・**
  ソフトウェア品質説明力強化の基本的な考え方の趣旨に沿った個別制度の企画、設計、運用および改善に対して責任を持つ組織

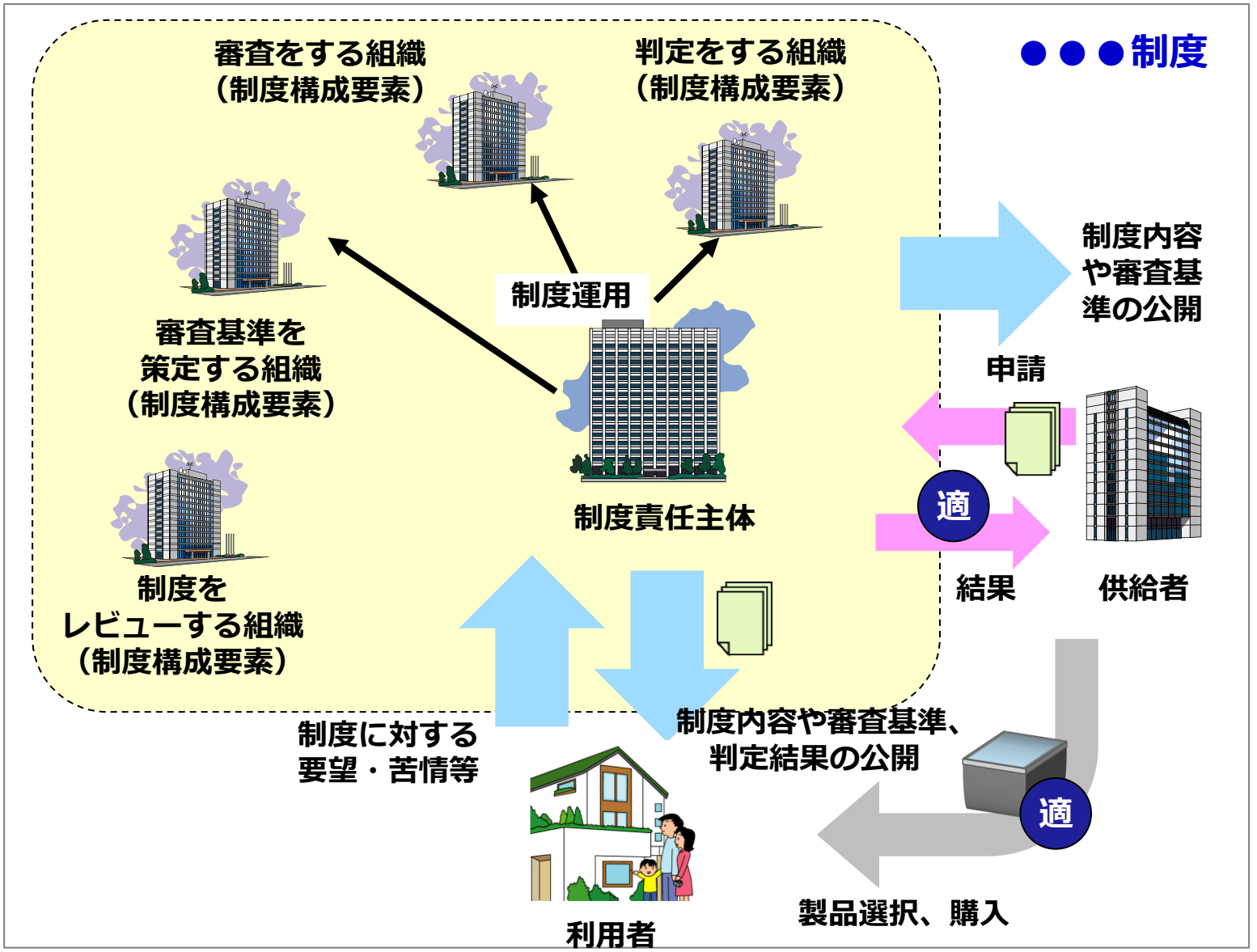
- **制度構成要素・・・**
  制度に必要な役割のうち、専門性や独立性が要求される一部の役割を担う組織。制度責任主体が事前に定義した要求事項に基づいて具体的な組織を決定

制度責任主体の役割



- ✓ **制度の企画**
- ✓ **制度の設計**
- ✓ **制度の運用**
- ✓ **制度の変更及び改善**

個別制度開発・運用の例


●●●制度
審査をする組織
（制度構成要素）
判定をする組織
（制度構成要素）
制度運用
審査基準を
策定する組織
（制度構成要素）
制度責任主体
制度を
レビューする組織
（制度構成要素）
制度内容
や審査基
準の公開
申請
適
結果
供給者
制度に対する
要望・苦情等
制度内容や審査基準、
判定結果の公開
適
製品選択、購入
利用者

制度ガイドラインが規定する要求事項

SEC Software Reliability Enhancement Center

個別制度に対する要求事項を以下カテゴリで定義

カテゴリ	概要	項目数
基本的な要求事項	制度の対象など、制度に対する基本的な要求事項（原則）	4
制度責任主体への要求事項	制度責任主体の組織や、企画・設計、運用・改善に関する事項	１７
制度規定に記述する項目	制度内容について策定した規定において、盛り込むべき（基本的に公開する）項目に関する事項	２２

本ガイドラインに基づく制度は、上記の要求事項を満足するものでなければならない。また、制度責任主体は、これらの要求事項以外に社会にとって有益な制度とするための取組みをすることが望ましい。

要求事項の例

SEC Software Reliability Enhancement Center

特に制度の公正性を担保する（審査機関の独立性や制度自身の第三者レビュー等を要求）ことを考慮して要求事項をまとめている。

4.1. 基本的な要求事項

制度に対する基本的な要求事項を表　4-1 に示す。

表 4-1 制度に対する基本的な要求事項

項番	分類	項目	要求事項
B-01	原則	対象（製品・システム）	製品・システムの重要な機能をソフトウェアで実現する場合の、その製品・システムを対
B-02		対象（品質）	
B-03		第三者による定	
B-04		判定結果の公	

表 4-2 制度責任主体に対する要求事項

項番	分類	項目	要求事項
E-01	組織	資格	制度責任主体は、法人格を持つこと。
E-02		経営資源	制度責任主体は、健全な制度運用に必要な経営資源（人、物、財）を持つこと。
E-03		責任	制度責任主体は、制度運用に対して責任体制を持つこと。
E-04	企画・設計	実施体制の設計	制度責任主体は、制度が必要とする機能を検討し、それを担う組織・要員の要求事項を規定すること。機能は以下を含む。 ・審査基準の策定・改善・管理 ・審査の実施 （必要な場合、審査の手段として）技術的な検証の実施 ・判定の実施 ・制度のレビュー 審査の実施者、及び判定の実施者は、供給者とは独立であること。 制度レビュー実施者は制度責任主体及び他の制度構成要素、供給者とは独立であること。 要求事項の例を付録に示す。
E-05		制度規定の策定	制度責任主体は、制度の運用に必要な規定を策定し、文書化すること。

表 4-3 制度内容規定に記述すべき項目

項番	記載項目	説明
基本事項		
R-01	制度の名称	制度の名称を示す。
R-02	目的等	制度の目的等を示す。利用者に対する制度の意義、供給者に対する制度の意義を含む。
R-03	適用範囲	制度の対象となる産業、製品・システムの適用範囲及び品質の範囲を示す。
R-04	制度の問合せ窓口	制度に関する一般からの問合せに対応するため、問合せのための連絡先を示す。
審査に関する事項		
R-05	審査基準の指定	審査に用いる審査基準を指定する。
判定に関する事項		
R-06	判定方法	審査結果等を基礎として適否の判定を行う方法を示す。
R-07	判定結果の有効性	判定結果に有効期間を設ける場合は、それを示す。また、製品・システム等のバージョンアップやカスタマイズ等の際の、以前の判定結果の有効性の有無を示す。
R-08	判定結果を適とした際の取扱	判定を適とした際の取扱い（適事実公開の方法、

制度ガイドラインの活用

SEC
Software Reliability Enhancement Center

制度責任主体（業界団体等）

制度企画 目的、対象範囲等の明確化

制度設計 リソースの確保、機能の設計、制度規程・運用規定等の作成、審査基準の定義、等

制度運用 運用、維持・管理

制度変更及び改善 関係者の要望反映、規格・法令への対応等

制度規定類等

「ソフトウェア品質説明のための制度ガイドライン」

要求事項に対する準拠性の確認

IPAがサポート

規定等に従った運用と改善

Copyright © 2013 IPA, All Rights Reserved

（ソフトウェア品質説明のための制度ガイドライン）
事例（PSQ認証制度）

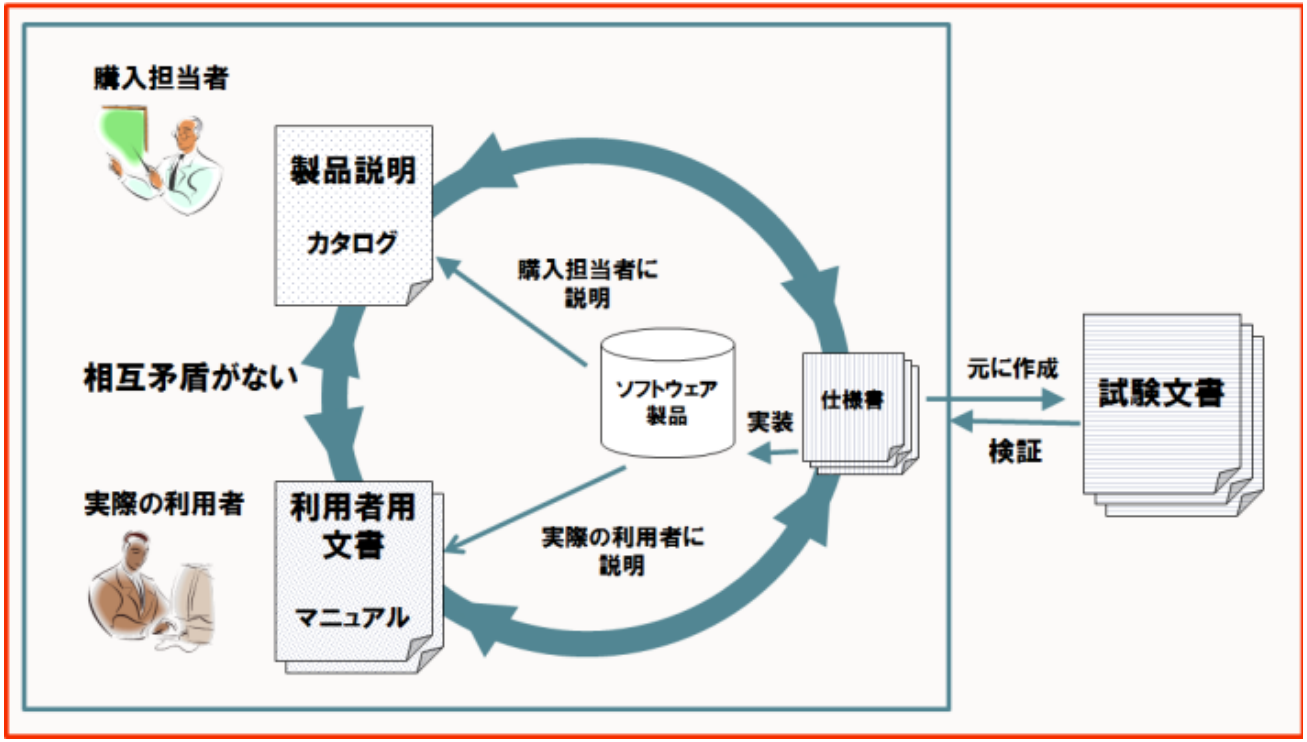
Copyright © 2013 IPA, All Rights Reserved

ソフトウェア品質説明力強化のための制度ガイドラインの展開
パッケージソフトウェア品質認証への展開：CSAJのPSQ認証の枠組み

SEC Software Reliability Enhancement Center

- パッケージソフトウェア製品を対象に、一般社団法人コンピュータソフトウェア協会（CSAJ）が創設した制度（パッケージソフトウェア品質認証制度）
- ソフトウェア製品の製品説明（カタログなど）、利用者用文書（マニュアルなど）がソフトウェア製品の機能と合致していることを第三者が確認し、CSAJが認証する制度

PSQ
Package Software
Quality Certification



一般社団法人コンピュータソフトウェア協会の資料を元に作成

Copyright © 2013 IPA, All Rights Reserved

PSQ認証制度とは

SEC Software Reliability Enhancement Center

＜製品に関する情報＞

・製品名
・バージョン 等

・想定利用者
・利用目的
・利用状況
・制約条件等

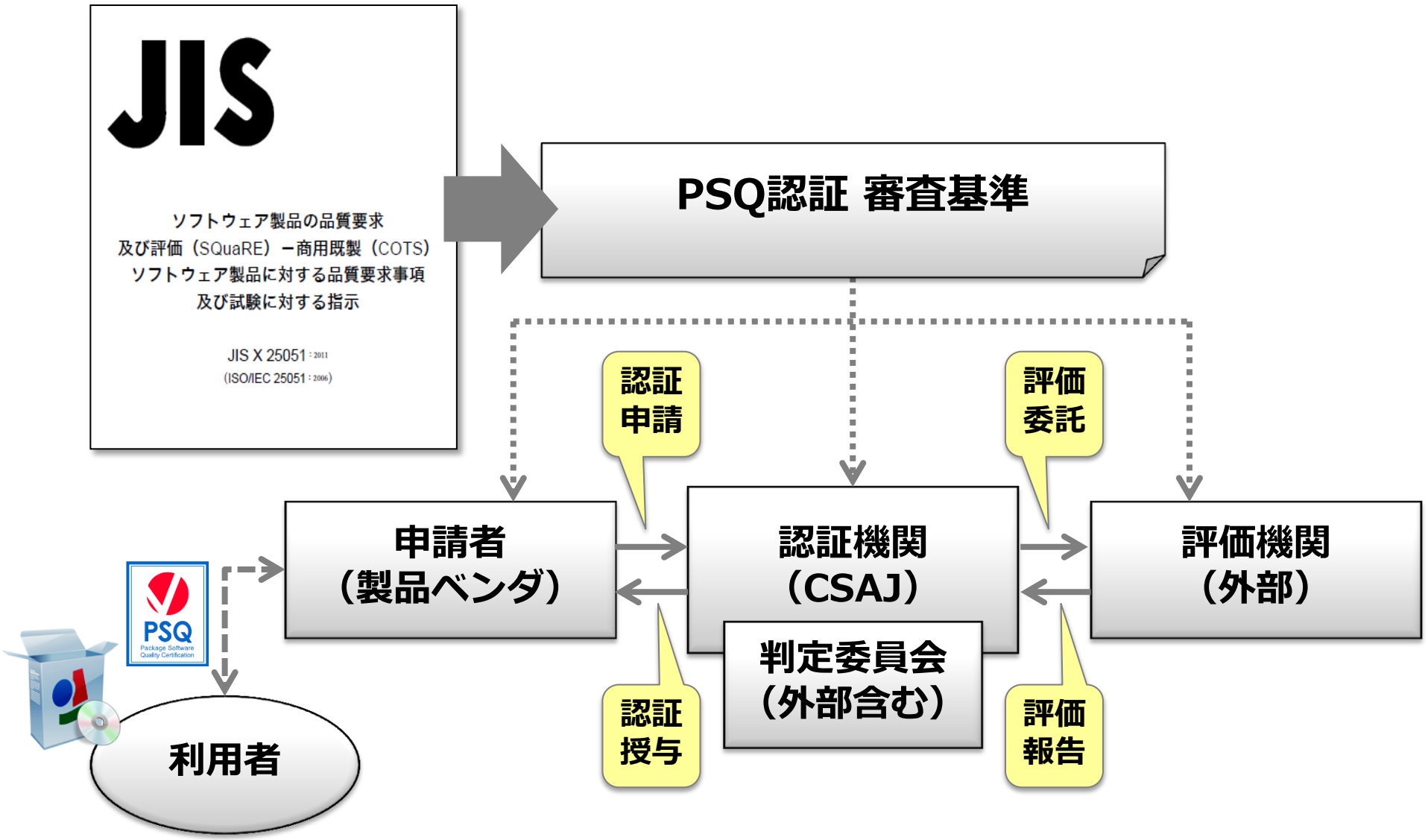
・品質目標
・製品の重要機能

審査基準

製品説明	利用者用文書	試験文書
カタログ、Webサイト、製品の外装表示等 製品購入の判断に使用	取扱説明書、オンラインヘルプ等 製品の利用時に使用	製品の機能に関わる 開発時のエビデンス

【各文書の品質・記載内容】　【各文書間のトレーサビリティ】
が規格（JIS X 25051）の要求事項を満たしているかを審査・認証

PSQ認証制度のスキーム



PSQ認証制度の審査基準

SEC
Software Reliability Enhancement Center

パッケージソフトウェア品質確認のための JIS X 25051に基づく審査基準

JIS

ソフトウェア製品の品質要求
及び評価（SQuaRE）ー商用既製（COTS）
ソフトウェア製品に対する品質要求事項
及び試験に対する指示

JIS X 25051：2011
(ISO/IEC 25051：2006)

平成23年1月20日 制定

日本工業標準調査会 審議

(日本規格協会 発行)

IPA 独立行政法人
Information-technolog

No.	審査基準項目	特記事項等
	合、それが明記されている。	
6	ソフトウェアを構成する要素が選択可能な場合、それが明記されている。	
8.4.2 信頼性		
1	エラー発生時の運用・操作の継続性が記載されている。	申請書中の各記載項目について、製品説明中の該当箇所にその内容が記載されており、一致していること。
2	データの退避手順、復元手順が記載されている。	
3	品質特性のうち「信頼性」に該当する事項がある場合、各副特性を考慮して記載されている。	
8.4.3 使用性		
1	ユーザインタフェースの種別が記載されている。	申請書中の各記載項目について、製品説明中の該当箇所にその内容が記載されており、一致していること。
2	アクセス容易性を考慮した製品の場合、アクセス容易性について記載されている。	

まとめ

まとめ

SEC Software Reliability Enhancement Center

■ 背景

- ✓ 一旦事故が起こると求められる品質説明
  ⇒第三者による客観性が大事
- ✓ 複雑化・高度化でソフト起因の障害は増加傾向？
  ⇒IT融合分野などますます品質説明が求められる
- ✓ 利用者にもITリテラシーが求められるが…
  ⇒専門家の第三者が利用者にわかりやすく示す

■ ソフトウェア品質説明とは？

- ✓ 品質説明の４つの要素
  ⇒①想定する利用者等、②利用する上で必要な品質目標、
  ③目標達成のための設計等、④目標を達成したことの検証等
- ✓ 説明力強化の３つの視点
  ⇒①技術的側面、②管理的側面、③制度的側面

■ ソフトウェア品質説明のための制度ガイドライン

⇒第三者が品質を確認し、利用者に示す制度を作る際の指針をまとめたもの
様々な分野での展開を図っていく

Copyright © 2013 IPA, All Rights Reserved

（ソフトウェア品質説明のための制度ガイドライン）
今後の展開

Copyright © 2013 IPA, All Rights Reserved

今後の展開

制度ガイドラインの認知度向上のための各種業界団体等への説明、製品やサービスが連携する新たな分野も含めニーズを把握し、制度化に向けての支援を実施

以下のニーズがある業界団体等

- 安全・安心につながる公正な情報提供により利用者の信頼を確保したい
- 品質の良い製品を流通させる仕組みを整備したい
- 国際標準や規制がない分野において客観性のある品質説明の基準を整備したい
- 障害発生時に品質に対する説明責任を果たせるようにしたい

ソフトウェア品質説明のための制度ガイドライン
第三者が品質を評価する制度が持つべき基本的な要件を規定

Copyright © 2013 IPA, All Rights Reserved

ご清聴ありがとうございました

IPA

＜PR＞

http://www.jitec.ipa.go.jp/ip/

Copyright © 2013 独立行政法人 情報処理推進機構